RECOMMENDED DOCUMENTATION FOR CLINIC PRIVACY AND SECURITY

Summary

This guide describes essential privacy and security documentation for a primary care clinic. Along with maintaining a library of digital records, create hard-copy binders easily accessible in case of major computer network failure.

Privacy and Security Binder Content

The Privacy and Security Binder should contain key information that is a foundation of personnel training and trusted information source for daily operations. It is an important part of your clinic security culture and can play an important role during a privacy breach investigation or when resolving complaints.

Both printed and digital documents of the Privacy and Security Binder should be well organized and easily available to ensure efficiency and transparency. The binder should include the following clearly marked sections:

Emergency contacts	Clinic's key contact information to assist in an emergency: ▪ Privacy Officer ▪ Security Lead ▪ EMR technical support ▪ Local IT Support Line ▪ Alarm Company ▪ Office of the Information and Privacy Commissioner ▪ Doctors Technology Office ▪ Other supporting organization
Clinic Privacy and Security Policies	Copies of all current policies with related appendices in separate, easy to find tabs.
Practice Procedures	This section should contain clearly marked procedures that are critical for emergency situations.
Responding to a Breach	A printed copy of the OIPC's document: "Privacy Breaches: Tools and Resources" Ensure to include the Privacy Breach Checklist found on page 11.
Training Materials	A list of materials that the clinic uses to train new staff and provide periodic Privacy and Security refreshers.
Useful References	For example: Physician Office IT Security Guide BC Physician Privacy Toolkit

IT Documentation, Procedures, and Logs

Documents listed below may contain sensitive information and both, electronic and paper copies, must be kept in a separate secure space. IT documentation is often technical in nature and generally maintained by IT support staff. Maintaining ongoing technical logs is important for ensuring the right level of safeguards have been implemented and is used for risk management, breach investigation, and problem resolution. Examples include:

Access Control	Information used to add and change user accounts on the clinic's systems. Updated copies should also be kept off-site in a secure location.
Technical Documentation	▪ An office map showing the physical location of equipment; ▪ Specifications, and purchase/warranty information for technology equipment; ▪ Software inventory: licences, certificates, renewal dates, and contacts; ▪ A network scheme showing connected clinic systems for rapid troubleshooting.
Technical Procedures	Current procedures used by IT staff to configure and maintain clinic IT systems, including system backups (see below), and those related to critical system logs.
Log Files:	
▪ System Backups	In addition to files generated electronically by backup applications, a printed or hand-written record should be kept for easy reference in case of major system failure. This log file might include the specific media label used, verification that the backup was successful, and where the media is currently located (on-site or off-site).
▪ System Logs	System logs are generally generated electronically by systems and as such kept online. Ensure the following logs are available: ▪ System performance monitoring and alerts ▪ User access
▪ Service Logs	A current and detailed record documenting changes to hardware and software. Examples include ▪ Adding, removing, and changing equipment and software ▪ Device disposal logs

HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

Other Office Administration Documents

The following documents are generally available to the Privacy Officer and designated staff.

Contracts and Agreements	▪ IT support contracts ▪ Staff and third-party confidentiality agreements ▪ Data sharing agreements, if applicable
Privacy Breaches	Completed Privacy Breach Checklist Forms, investigation and submitted reports.
Privacy Training	Records of privacy training with content, attendance list, and session date.
Privacy Impact Assessments (PIAs)	When possible, complete a self-assessment for newly implemented technology and major system changes.

DISCLAIMER

This document provides general guides and approaches only. We strongly recommend that you retain a knowledgeable and qualified professional to regularly assess and maintain your clinic's technology.

For more information, guidance, or support contact:

Doctors Technology Office
604 638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office